IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Aguro	Docket No.:	TI-26495
Serial No.:	09/281,042	Art Unit:	2123
Filed:	03/30/1999	Examiner:	Jones, H.
For:	COMPUTER SYSTEM		

APPEAL BRIEF TRANSMITTAL FORM

MAILING CERTIFICATE UNDER 37 C.F.R. §1.8(A)

I hereby certify that the above correspondence is being deposited with the US Postal Service as First Class Mail in an envelope addressed to: Assistant Commissioner for Patents, Washington, DC 20231

William B. Kempler 2/19/02
Date

Assistant Commissioner For Patents
Washington, DC 20231

Sir:

Transmitted herewith in triplicate is an Appeal Brief in connection with the above-identified application.

Please charge $320.00 fee for filing the Brief to Deposit Account No. 20-0668.

To the extent necessary, the Applicants petition for an Extension of Time under 37 CFR 1.136. Please charge any additional fees in connection with the filing of this paper, including extension of time fees, to Deposit Account No. 20-0668 of Texas Instruments Incorporated.

Respectfully submitted,

Texas Instruments Incorporated
P. O. Box 655474, MS 3999
Dallas, Texas 75265
(972) 917-5452

William B. Kempler
Senior Corporate Patent Counsel
Reg. No. 28,228

#19
cc
3/27/02

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Seiki Aguro	Docket No.:	TIJ-26495
Serial No.:	09/281,042	Art Unit:	2123
Filed:	03/30/1999	Examiner:	Jones, H.
For:	COMPUTER SYSTEM		

APPEAL BRIEF

Assistant Commissioner for Patents
Washington, DC 20231

Dear Sir:

The following Appeal Brief is respectfully submitted in support of an appeal of the final rejection of Claims in connection with the above-identified application. The final Rejection was mailed 6/19/2001, and the Advisory Action mailed 10/23/2001.

REAL PARTY IN INTEREST

The invention has been assigned to Texas Instruments Incorporated.

RELATED APPEALS AND INTERFERENCES

There are no appeals or interferences known to Applicant's representative which will directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

STATUS OF THE CLAIMS

UNKNOWN. Claims 1-3 were filed with the application and amended on filing by a preliminary amendment. Claims 1-3 were cancelled by the amendment dated 03/26/2001 and were replaced by new Claims 4-21. Claims 4-21 were rejected in the final rejection of 06/19/2001. Claims 4 and 8 were amended in the amendment dated 10/01/2001. In the Advisory Action of 10/23/2001 the Examiner complained that a "marked up copy" was not provided although one was submitted with the 10/01/2001 amendment. A copy of the marked up version of the Claims was sent along with the Notice of Appeal with a request that the amended Claims be entered because they only corrected typographical errors and were therefore in a better form for appeal. No response has been received. The Advisory Action indicated that the Examiner accepted none of Applicant's arguments but indicated, that on filing an Appeal, Claims 4-21 are allowed.

Accordingly, Applicant cannot ascertain the status of the Claims from the record. Claims 4-21, including Claims 4 and 8 as amended, should be the Claims on appeal.

STATUS OF THE AMENDMENTS

The application was filed with Claims 1-3, which were amended on filing by a preliminary amendment. These Claims were cancelled by the amendment dated 03/26/2001 and replaced by Claims 4-21. Claims 4 and 8 were amended in an amendment dated 10/01/2001, which amendment was not entered by the Examiner.

SUMMARY OF THE INVENTION

The present invention is related to preventing access to the program stored within a one-chip computer system. It is common to provide security for a computer system via a password and a limitation on the number of tries to input the correct password. This works in a fixed system environment. In a one-chip computer environment, this method will fail

because there is a large number of systems available on which attempts for unauthorized access may be tried.

The present invention provides a simple yet effective solution to the problem by having the processor utilize a stored program to receive and process a plurality of commands applied to a plurality of input ports to the processor to generate the password (page 14, lines 3-25, page 15, lines 8-23 and page 16, lines 15-23). This permits the commands to be applied in a described sequence, which makes cracking the password far more difficult without the necessity of complex circuitry dedicated to security.

ISSUES

The issues on appeal are whether the Examiner's requirement that Applicant cite references in an IDS are valid, whether his statements that the present invention is shown in IEEE Standard 1149.1 are correct, whether there is sufficient support in the application for Claims 4-20 under 35 U.S.C. § 112, first paragraph, whether Claims 8, 10 and 14-15 omit both an essential step and an essential structural cooperative element, whether the recitation in Claim 4 can meet the requirements of 35 U.S.C. § 112, second paragraph with regards to the essential step/essential cooperative element rejection, but the identical recitation in Claim 8 fails to meet this requirement, whether Claims 8-21 are anticipated by Curd et al. and whether the Examiner's inconsistent and self-contradictory statements place an unreasonable burden on Applicant.

GROUPING OF THE CLAIMS

Each of the following groups of Claims, as contained in the attached Appendix, are independently patentable, and the rejected Claims of these groups stand or fall together for the reasons more clearly set forth hereinbelow:

Group I	4-7
Group II	8-13
Group III	14-21

ARGUMENTS

Information Disclosure Statement

The Examiner states that "Applicant has referred to scan circuits and ICE systems in the Background of the Invention, but has not provided an IDS . . . . Applicant has also admitted that Fig. 4 represents a prior art teaching - thus, admitting that Applicant is aware of specific prior art teachings. Furthermore, Applicant's invention has been disclosed as part of IEEE Standard 1149.1. It is presumed that Applicant is of at least ordinary skill in the art and therefore presumably aware of said standard.". In the Official Action of 10/24/2000, the Examiner asked if the Representative was aware of other relevant art. In the Final Rejection of 06/19/2001, the Examiner stated that "the Applicant should provide the office with copies of pertinent art in any response to this action.".

Applicants traverse the Examiner's statements regarding the requirements for an IDS and regarding the Standard. Even the Examiner does not believe his statement regarding the Standard and has admitted that the present invention is not shown in the IEEE Standard. In the first Official Action, dated October 24, 2000, the Examiner cited this Standard as prior art made of record and not relied upon. Therefore, the Examiner's Action contradicted his own statements. Furthermore, in the Final Rejection, the Examiner did not reject even a single Claim in view of this Standard. Therefore, it is clear that the Examiner does not believe his own statements that the invention has been disclosed as part of the Standard.

This is one of the many self-contradicting statements made by the Examiner during the prosecution of this application which has led to this appeal.

The requirement for the duty of disclose information material to patentability is found in 37 CFR § 1.56 and the requirements for an IDS are found in 37 CFR § 1.97 and 1.98. Under 37 CFR § 1.56, information to be cited in "information known to that individual to be material to patentability as defined in this section". 37 CFR § 1.56(b) defines information that is material to patentabiity as not being cumulative to information already of record or being made of record and "(1) It establishes, by itself or in combination with other information, a *prima facie* case of unpatentability of the Claim; or (2) It refutes or is inconsistent with, a position the Applicant takes in:

(i) Opposing an argument of unpatentability relied on by the Office, or

(ii) Asserting an argument of patentability."

The Examiner has argued that the IEEE Standard is a reference that Applicant should have cited in an IDS. However, it is clear from the Examiner 's actions that this reference does not meet the requirements for materiality discussed above. The Examiner did not apply this reference against any Claim in either Official Action nor use the Standard to reject any argument for patentability or reject any argument opposing an argument for unpatantability relied on by the Office that Applicant has made. Therefore, the Examiner, by his actions, has shown that this reference is not material to the invention defined by the present or the cancelled Claims. The Examiner also alludes to the Background of the Invention section and Figure 4 of the present application. The inventor informs us that Figure 4 is not taken from the IEEE Standard because the Standard has no description of the emulation logic, but is an abstract image of emulation logic and scan-path interface logic accessed by an emulator. An IDS requires the citation of a specific reference.

Secondly, the Examiner states that he is aware of and obtained numerous examples of such teachings. Applicant is pleased that the Examiner has performed a thorough search of the art as that is the only way they will receive a strong patent. However, finding these references is the Examiner's job and not Applicant's. Furthermore, the Examiner has signed the Official Actions as "Dr." which presumably means he has a Ph D. Accordingly, even if he thinks that the inventor is of ordinary shell in the art, he may

be at a much higher level, which should not be used to place additional burdens on Applicant or draw negative inferences therefrom.

Applicants did submit an IDS containing two references that the inventor searched for, in the Response to the Final Rejection.

35 USC § 112, first paragraph rejection

The Examiner rejects Claims 4-21 as containing subject matter not described in the specification in such a way as to enable one skilled in the art to make and/or use the invention. This rejection was first raised in the Final Rejection and was based on Applicant's failing to specifically point out support in the specification for the amendments.

Support for the amendments was made in the Response mailed on March 26, 2001 was included in the Response to the final rejection mailed on October 01, 2001. The Examiner did not enter this Response.

35 USC § 112, second paragraph rejection

The Examiner rejects Claims 8, 10, and 14-15 as being incomplete for omitting essential steps, such omission amounting to a gap between the steps. The Examiner rejects the same Claims as being incomplete for omitting essential structural cooperative relationships of elements, such omission amounting to a gap between necessary structural connections.

The Examiner has not made these rejections in the alternative. Accordingly Claims 8, 10 and 14-15 are rejected for omitting essential steps and essential cooperative relationships of elements. The former are found in method claims, the later in structure claims. The Examiner does not allege that there are method steps in a structure claim or structural relationships in a method claim. Therefore only one or the other rejection is proper, and one of the rejections is improper. The Examiner ignored this in the Advisory

Action. This is another portion of the final rejection that is self-contradictory which rendered this appeal necessary.

For the record, and as stated in the Response mailed October 01, 2001, Claim 8 is a subcombination Claim, Claim 14 is a system Claim and Claims 10 and 15 are dependent on Claims 8 and 14, respectively. Accordingly, these Claims are all structural Claims and not method Claims. it is for this reason that the Examiner cannot find method steps in these Claims, as is appropriate.

With respect to the Claims being incomplete for omitting essential structural cooperative relationships of the elements, Applicants are confused because the statement is in direct contradiction to the Examiner's statement in paragraph 11 in which Claims 4-7 are deemed novel and non-obvious over the prior art and being allowed when all outstanding deficiencies are traversed. Since these Claims were omitted from the 35 USC § 112, second paragraph rejection, it means that the Examiner found these Claims to meet the requirements of that paragraph. Claim 4 (As amended to correct a typographical error) recites in pertinent part:

". . . security means comprising

a plurality of input ports for said processor;

a program stored in said memory to operate said processor to receive a plurality of commands applied to said plurality of input ports and to process said commands to produce a password which is compared with a predetermined password.".

Claim 8 (as amended to correct a typographical error) recites in pertinent part:

". . . a security system comprising:

a plurality of input ports for said processor;

a program stored in said memory to operate said processor to receive a plurality of commands applied to said plurality of input ports and to process said commands to produce a password which is compared with a predetermined password.".

Claim 14 recites:

"A security system for an integrated circuit computer system comprising:

means for applying a plurality of commands to a plurality of ports for a processor of said system;

a program stored in a memory coupled to said processor for operating said processor to process said plurality of commands to produce a password;

means for comparing said produced password with a predetermined password.".

If one compares the description of the security system described in Claim 8 and the security means described in Claim 4, one finds that the description is identical. Claim 14 which claims the security system utilizes a very similar recitation of the elements. Accordingly, Applicants wonder how the descriptions can be acceptable in the allowed Claim 4 but not acceptable in Claims 8 and 14.

The contradiction in the Examiner's acceptance of the language in Claim 4 while rejecting the identical language in Claim 8 and very similar language in Claim14 is another of the self-contradictory statements made by the Examiner which necessitates this appeal.

Applicants submit that there is sufficient description in all of the Claims to meet the 35 USC § 112, second paragraph, requirement. For example, Claims 4 and 8 both recite a plurality of input ports for the processor. In Claim 14 the recitation is for means for applying a plurality of commands to a plurality of ports for a processor. Clearly those skilled in the art know how a signal applied to an input port of a processor is received by the processor and no further description is necessary. Next, the Claims recite a program stored in the memory to operate the processor to receive a plurality of commands applied to a plurality of input ports and to process the commands to produce a password. Those skilled in the art know how a computer program can receive data on input ports of a processor and process the data to generate a password. Thus, this need not be described in detail. Next is the recitation of the comparison of a password with a predetermined password, and this feature is shown in Figure 3 of the reference Curd et al. cited by the Examiner, and

therefore is known in the art and need not be further described. Accordingly, Applicants submit that all the elements are properly recited in sufficient detail to meet the requirements of 35 USC § 112, second paragraph.

Rejection under 35 USC § 102

Claims 8-21 stand rejected under 35 USC § 102(e) as being clearly anticipated by Curd et al. of record. The Examiner states that Curd et al. discloses overridable data protection mechanism for PLDs and refers to the abstract; Fig. 1-3; col. 1, line 45 to col. 2, line 50. The Examiner states that it should be noted that Figure 3 discloses two separate inputs which are then compared.

This rejection is respectfully traversed. The present invention is not anticipated by or obvious over Curd et al. In order for rejection under section 102 to apply, all the elements of the present invention must be shown in the cited reference. Firstly, Claim 8 recites a processor interconnected with a memory and peripheral circuit on the integrated circuit. In Curd et al., the processor is in a computer system which is connected with the integrated circuit when it is time to program the integrated circuit. There is no processor on the integrated circuit, and thus a section 102 rejection must fail. Secondly, Claim 8 recites a program stored in a memory to operate the processor to receive a plurality of commands applied to a plurality of input ports and process the commands to produce a password. Since there is no processor at all on the chip, there can be no program used to operate a processor. Furthermore, the Examiner's statement to the contrary notwithstanding, Figure 3 does not disclose two separate inputs which are compared. The input key register 302 is an input to the system which is compared with the data protect overwrite register key 301, which is data already contained in the system and thus not input into the system. It is true that both these registers are applied as inputs to the comparitors, but this is true of any comparitor.

Inconsistent and self-contradictory statements made by the Examiner

The prosecution of this application is replete with inconsistent statements made by the Examiner which are often self-contradictory. This makes it impossible for Applicants to prosecute the application in a reasonable manner.

The status of the Claims is listed herein as "unknown" because the Examiner first refused to accept any of the arguments in our response to the final rejection, but listed all of the Claims as allowed on filing an appeal. Clearly all of the Claims cannot be allowed or there are no Claims to appeal.

The Examiner stated that the invention is disclosed in the IEEE Standard that he cites, yet not even a single Claim has been rejected based on this art. Clearly, even the Examiner does not believe his own statements.

The Examiner rejects Claims 8, 10 and 14-15 under 35 USC § 112, second paragraph both for omitting essential steps and for omitting essential structural cooperative relationships of elements, thus stating that the Claims contain both method steps and structural elements. Does the Examiner believe the Claims to be method Claims or structural Claims? Or is the Examiner stating that the Claims area hybrid of both? The Claims in question contain NO method steps because they are structure Claims. At least one of these two rejections must fail. Why does Applicant have to guess which one?

Furthermore, the language in Claim 8 that the Examiner rejects is identical to the language in Claim 4 which the Examiner states is allowable. Not only does this confuse Applicant on the Examiner's position, but it places a statement in the file history which would make an allowed Claim 4 of dubious value. Thus, even if Applicant desired to accept the Claims 4-7 which the Examiner found allowable, it would not be appropriate to do so.

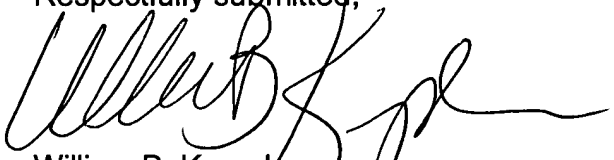
We believe that an unreasonable burden has been placed on Applicants by the Examiner's actions. Applicant should not be in a position of having to take a first action based on the Examiner's first statement only to achieve a dubious result based on his second statement. Although Applicant and the Examiner may disagree on points in an action, at least Applicant should be able to rely on the clear meaning of the Examiner's statements.

Applicant raised these issues in their Response to the Final Rejection. The Examiner responded to each in the Advisory Action by a single sentence statement stating that Applicants concerns are "not accepted" by the Examiner, thus necessitating this appeal.

CONCLUSION

For the above reasons, Applicants respectfully submit that the Examiner's Final Rejection of Claims 4-21 under 35 U.S.C. § 102, 35 U.S.C. § 112, first paragraph, 35 U.S.C. § 112, second paragraph and the Examiner's statements and requirements with regard to an IDS are not properly founded in law. Applicants respectfully request that the Board of Patent Appeals and Interferences so find and reverse the Examiner's rejections of the Claims and his statements and requirements with regard to an IDS.

Respectfully submitted,



William B. Kempler
Senior Corporate Patent Counsel
Reg. No. 28,228

Texas Instruments Incorporated
P.O. Box 655474, MS 3999
Dallas, TX 75265
(972) 917-5339

APPENDIX

Version 1 with typographical errors in Claims 4 and 8.

4. An integrated circuit computer system comprising:

a processor interconnected with memory and peripheral circuits on said integrated circuit;

a scan-path interface circuit for reading out contents of a predetermined memory or register in said system;

a switching circuit coupled to said processor and to said scan-path interface circuit for switching said scan-path interface circuit between a first mode in which it is enabled and a second mode in which it is disabled; and

security means comprising:

a plurality of input ports for said processor;

a program stored in said memory to operate said process to receive a plurality of commands applied to said plurality of input ports and to process said commands to produce a password which is compared with a predetermined password;

and wherein said switching circuit is responsive to said comparison.

5. The computer system of claim 4 wherein said program operates said processor to receive said plurality of commands which are applied to said plurality of ports in a specific time sequence.

6. The computer system of claim 4 further comprising a pair of registers, one of said registers receiving said produced password and the other of said registers containing said predetermined password; and a comparator for comparing the contents of said registers for controlling said switching circuit.

7. The computer system of claim 5 further comprising a pair of registers, one of said registers receiving said produced password and the other of said registers

containing said predetermined password; and a comparator for comparing the contents of said registers for controlling said switching circuit.

8. In an integrated circuit computer system having a processor interconnected with memory and peripheral circuits on said integrated circuit and coupled to a scan-path interface circuit, a security system comprising:

a plurality of input ports for said processor;

a program stored in said memory to operate said processor to received a plurality of commands applied to said plurality of input ports and to process said commands to produce a password which is compared with a predetermined password.

9. The security system of claim 8 further comprising a switching circuit coupled to said scan-path interface circuit and responsive to said comparison for switching said scan-path interface circuit between a first mode in which it is enabled and a second mode in which it is disabled.

10. The security system of claim 8 wherein said program operates said processor to receive said plurality of commands which are applied to said plurality of ports in a specific time sequence.

11. The security system of claim 8 further comprising a pair of registers, one of said registers receiving said produced password and the other of said registers containing said predetermined password; and a comparator for comparing the contents of said registers for controlling said switching circuit.

12. The security system of claim 9 further comprising a pair of registers, one of said registers receiving said produced password and the other of said registers containing said predetermined password; and a comparator for comparing the contents of said registers for controlling said switching circuit.

13. The security system of claim 10 further comprising a pair of registers, one of said registers receiving said produced password and the other of said registers containing said predetermined password; and a comparator for comparing the contents of said registers for controlling said switching circuit.

14. A security system for an integrated circuit computer system comprising:

means for applying a plurality of commands to a plurality of ports for a processor of said system;

a program stored in a memory coupled to said processor for operating said processor to process said plurality of commands to produce a password;

means for comparing said produced password with a predetermined password.

15. The security system of claim 14 wherein said program operates said processor to receive said plurality of commands which are applied to said plurality of ports in a specific time sequence.

16. The security system of claim 14 further comprising a pair of registers, one of said registers receiving said produced password and the other of said registers containing said predetermined password; and a comparator for comparing the contents of said registers and generating a comparison signal.

17. The security system of claim 15 further comprising a pair of registers, one of said registers receiving said produced password and the other of said registers containing said predetermined password; and a comparator for comparing the contents of said registers and generating a comparison signal.

18. The security system of claim 14 further comprising a scan-path interface circuit for reading out contents of a predetermined memory or register in said system and a switching circuit responsive to said comparison to switch operation of said scan-path interface circuit between enabled and disabled modes.

19. The security system of claim 15 further comprising a scan-path interface circuit for reading out contents of a predetermined memory or register in said system and a switching circuit responsive to said comparison to switch operation of said scan-path interface circuit between enabled and a disable modes.

20. The security system of claim 16 further comprising a scan-path interface circuit for reading out contents of a predetermined memory or register in said system and a switching circuit responsive to said comparison to switch operation of said scan-path interface circuit between enabled and a disable modes.

21. The security system of claim 17 further comprising a scan-path interface circuit for reading out contents of a predetermined memory or register in said system and a switching circuit responsive to said comparison to switch operation of said scan-path interface circuit between enabled and a disable modes.

Version 2 with typographical errors corrected

4. An integrated circuit computer system comprising:

a processor interconnected with memory and peripheral circuits on said integrated circuit;

a scan-path interface circuit for reading out contents of a predetermined memory or register in said system;

a switching circuit coupled to said processor and to said scan-path interface circuit for switching said scan-path interface circuit between a first mode in which it is enabled and a second mode in which it is disabled; and

security means comprising:

a plurality of input ports for said processor;

a program stored in said memory to operate said processor to receive a plurality of commands applied to said plurality of input ports and to process said commands to produce a password which is compared with a predetermined password;

and wherein said switching circuit is responsive to said comparison.

5. The computer system of claim 4 wherein said program operates said processor to receive said plurality of commands which are applied to said plurality of ports in a specific time sequence.

6. The computer system of claim 4 further comprising a pair of registers, one of said registers receiving said produced password and the other of said registers containing said predetermined password; and a comparator for comparing the contents of said registers for controlling said switching circuit.

7. The computer system of claim 5 further comprising a pair of registers, one of said registers receiving said produced password and the other of said registers

containing said predetermined password; and a comparator for comparing the contents of said registers for controlling said switching circuit.

8. In an integrated circuit computer system having a processor interconnected with memory and peripheral circuits on said integrated circuit and coupled to a scan-path interface circuit, a security system comprising:

a plurality of input ports for said processor;

a program stored in said memory to operate said processor to receive a plurality of commands applied to said plurality of input ports and to process said commands to produce a password which is compared with a predetermined password.

9. The security system of claim 8 further comprising a switching circuit coupled to said scan-path interface circuit and responsive to said comparison for switching said scan-path interface circuit between a first mode in which it is enabled and a second mode in which it is disabled.

10. The security system of claim 8 wherein said program operates said processor to receive said plurality of commands which are applied to said plurality of ports in a specific time sequence.

11. The security system of claim 8 further comprising a pair of registers, one of said registers receiving said produced password and the other of said registers containing said predetermined password; and a comparator for comparing the contents of said registers for controlling said switching circuit.

12. The security system of claim 9 further comprising a pair of registers, one of said registers receiving said produced password and the other of said registers containing said predetermined password; and a comparator for comparing the contents of said registers for controlling said switching circuit.

13. The security system of claim 10 further comprising a pair of registers, one of said registers receiving said produced password and the other of said registers containing said predetermined password; and a comparator for comparing the contents of said registers for controlling said switching circuit.

14. A security system for an integrated circuit computer system comprising:

means for applying a plurality of commands to a plurality of ports for a processor of said system;

a program stored in a memory coupled to said processor for operating said processor to process said plurality of commands to produce a password;

means for comparing said produced password with a predetermined password.

15. The security system of claim 14 wherein said program operates said processor to receive said plurality of commands which are applied to said plurality of ports in a specific time sequence.

16. The security system of claim 14 further comprising a pair of registers, one of said registers receiving said produced password and the other of said registers containing said predetermined password; and a comparator for comparing the contents of said registers and generating a comparison signal.

17. The security system of claim 15 further comprising a pair of registers, one of said registers receiving said produced password and the other of said registers containing said predetermined password; and a comparator for comparing the contents of said registers and generating a comparison signal.

18. The security system of claim 14 further comprising a scan-path interface circuit for reading out contents of a predetermined memory or register in said system and a switching circuit responsive to said comparison to switch operation of said scan-path interface circuit between enabled and disabled modes.

19. The security system of claim 15 further comprising a scan-path interface circuit for reading out contents of a predetermined memory or register in said system and a switching circuit responsive to said comparison to switch operation of said scan-path interface circuit between enabled and a disable modes.

20. The security system of claim 16 further comprising a scan-path interface circuit for reading out contents of a predetermined memory or register in said system and a switching circuit responsive to said comparison to switch operation of said scan-path interface circuit between enabled and a disable modes.

21. The security system of claim 17 further comprising a scan-path interface circuit for reading out contents of a predetermined memory or register in said system and a switching circuit responsive to said comparison to switch operation of said scan-path interface circuit between enabled and a disable modes.